

Smashing iOS Apps for Fun and Profit

Dark Luo & Sung-ting Tsai

{dark,tt}@chroot.org



關於我們



CHROOT



Dark Luo

社群

CHROOT – 成員

PHATE – 建立

Zuso Security – 成員

興趣

Reverse engineering & programming

RAT & Anti-Virus & Anti-Anti-Virus & Game
cheat engine

演講經歷

HITCON 2012 - iOS Hacking

HITCON 2009 - Game Hacking & Game
Protection Bypassing (Hackshield)

ZCamp 2008 - Reverse engineering



Sung-ting Tsai (TT)

趨勢科技

Leader of an advanced threat research team.

Core Tech Department

演講經歷

Black Hat USA 2011 / 2012

Codegate 2012

Syscan 10'

HITCon 08'

研究

New security technology

Malicious document

Malware auto-analyzing system (sandbox technologies)

Malware detection

System vulnerability and protection

Mobile security



內容

iOS Hacking



For Profit



For Fun





0x01:

Hacking iOS Apps

Analyzing Tools
Debug Tricks

iOS Apps

Mach-O 格式

Mach-O, short for Mach object file format, is a file format for executables, object code, shared libraries, dynamically-loaded code, and core dumps.

iOS and Mac OS X .

匯編語言

Arm V6 – Thumb

Arm V7 – Thumb v2

工具

一支 JB 過的 iPhone

第一步

GDB

動態分析

IDA Pro

靜態分析

otool

執行檔分析

class-dump

從執行檔取出標頭檔



iOS Apps 加密還原 (逆向分析之前你要先處理加密的部分)



找到加密的區段

```
# otool -l filepath | grep 'crypt'
```



使用 GDB 把程式跑起來



匯出解密後的區段



寫回 App 中



之後就可以使用 IDA Pro 分析

iOS Apps 加密還原

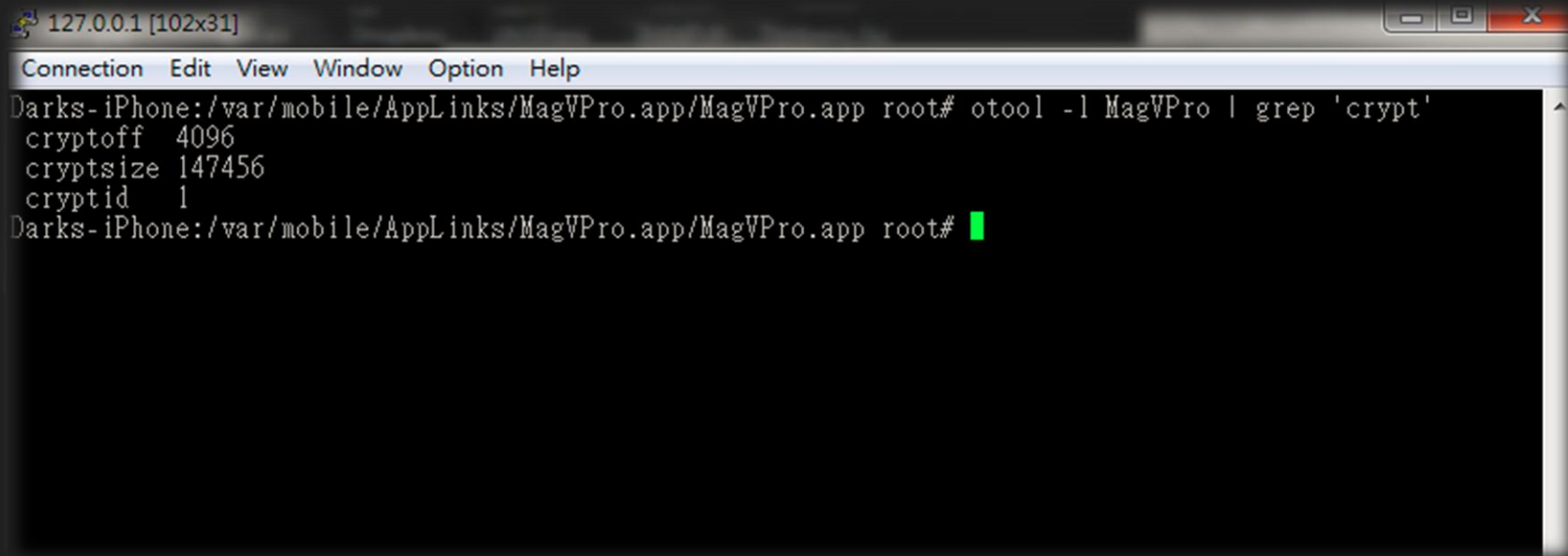


iOS Apps 加密還原 (1)

```
text:00002574 ;
text:00002574 ; =====
text:00002574 ; Segment type: Pure code
text:00002574 AREA __text, CODE, READWRITE
text:00002574 ; ORG 0x2574
text:00002574 CODE32
text:00002574 EXPORT start
text:00002574 start
text:00002574 LDCGE p9, c12, [R6], #0x14
text:00002578 BLLE 0xFF746890
text:0000257C SBCNE R3, R12, R0, LSL R2
text:00002580 LDHIB R7!, {R1-R7, R11, LR}^
text:00002584 STMVSI B R2, {R0-R5, R7, R8, R10, R12, LR, PC}^
text:00002588 MOVPL R11, 0xFF3BFFFF
text:0000258C SUCCE 0xC92D71
text:00002590 SUCGT 0xF47BF1
text:00002594 ORRNES R6, R10, #0x2A
text:00002598 STCLTL p0, c14, [SP, #0x26C]
text:0000259C LDRB LR, [PC, R4, ASR#26]!
text:000025A0 BLPL 0xFE51BD5C
text:000025A0 ; CODE XREF: -[&Vm_____ $ _1 _L _5 _0 _____ 9k _K _1 _5 _:_ W
text:000025A4 BCC 0xFE71BC94
text:000025A8 LDRHIBT R4, [R2], R1, LSL#12
text:000025AC UNAALEQS R5, R3, R10, R10
text:000025B0 MCRHI p9, 2, R4, c14, c9, 2
text:000025B4 STCUCL p6, c9, [R1], #-0x298
```

0001574: 00002574: text: start

iOS Apps 加密還原 (2)



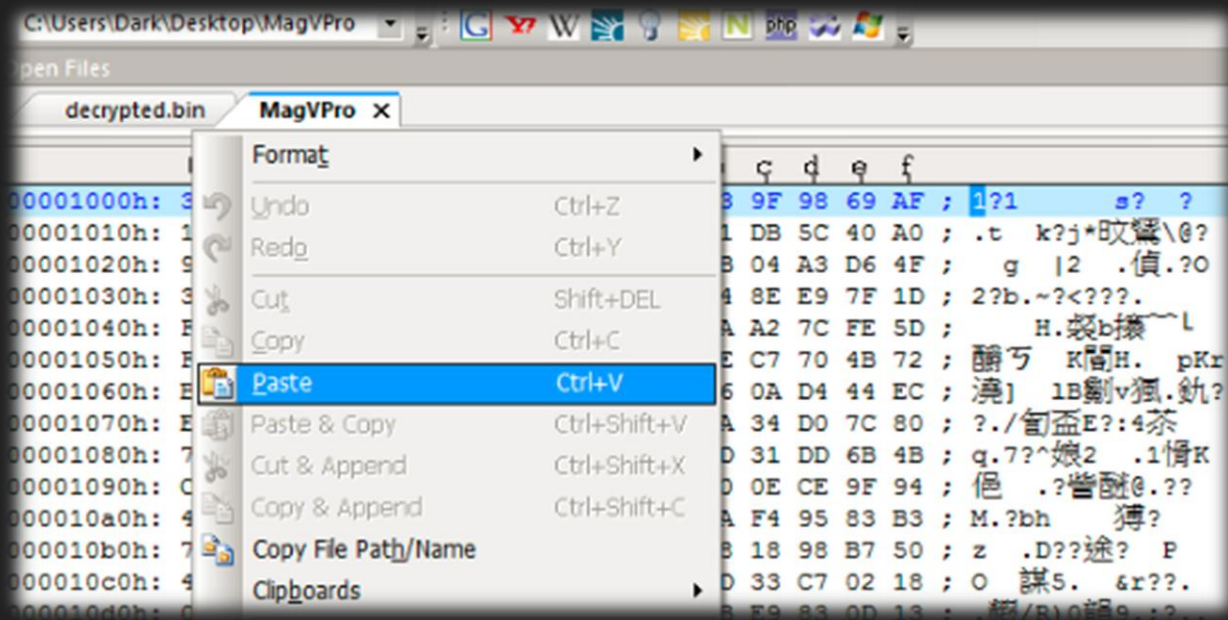
A terminal window titled '127.0.0.1 [102x31]' with a menu bar containing 'Connection', 'Edit', 'View', 'Window', 'Option', and 'Help'. The terminal shows a shell prompt 'Darks- iPhone:/var/mobile/AppLinks/MagVPro.app/MagVPro.app root#' followed by the command 'otool -l MagVPro | grep 'crypt''. The output is displayed on three lines: 'cryptoff 4096', 'cryptsize 147456', and 'cryptid 1'. The prompt is repeated on the next line with a green cursor.

```
127.0.0.1 [102x31]
Connection Edit View Window Option Help
Darks- iPhone:/var/mobile/AppLinks/MagVPro.app/MagVPro.app root# otool -l MagVPro | grep 'crypt'
cryptoff 4096
cryptsize 147456
cryptid 1
Darks- iPhone:/var/mobile/AppLinks/MagVPro.app/MagVPro.app root#
```

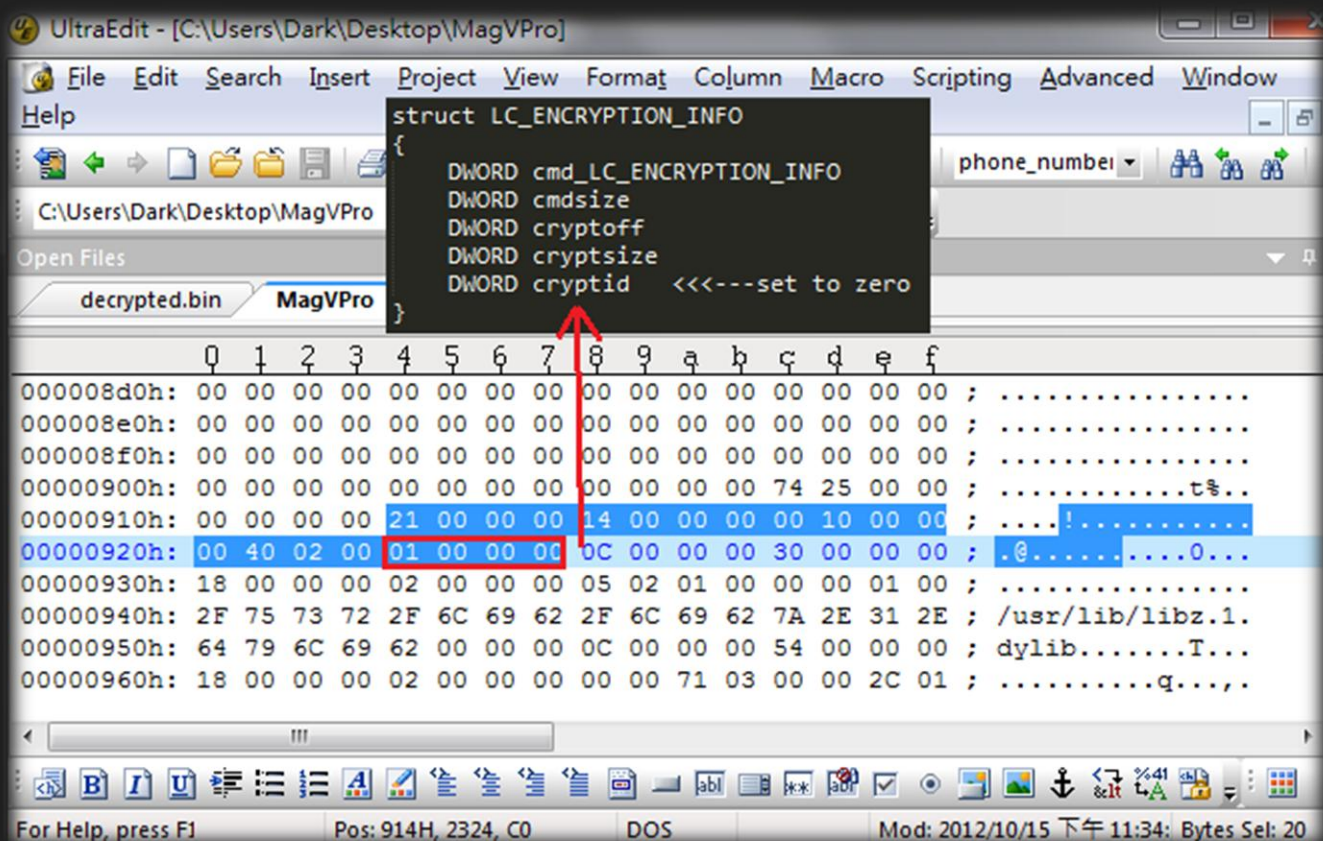
iOS Apps 加密還原 (3)

```
(gdb) run
Starting program: /private/var/mobile/Applications/99008E31-BDAD-402F-AB29-CFB5A74EF544/MagVPro.app/Ma
gVPro
Removing symbols for unused shared libraries . done
Reading symbols for shared libraries .....+++.....
..... done
^C
Program received signal SIGINT, Interrupt.
0x315a9004 in mach_msg_trap ()
(gdb) dump memory decrypted.bin 0x2000 0x2000+147456
(gdb) █
```

iOS Apps 加密還原 (4)

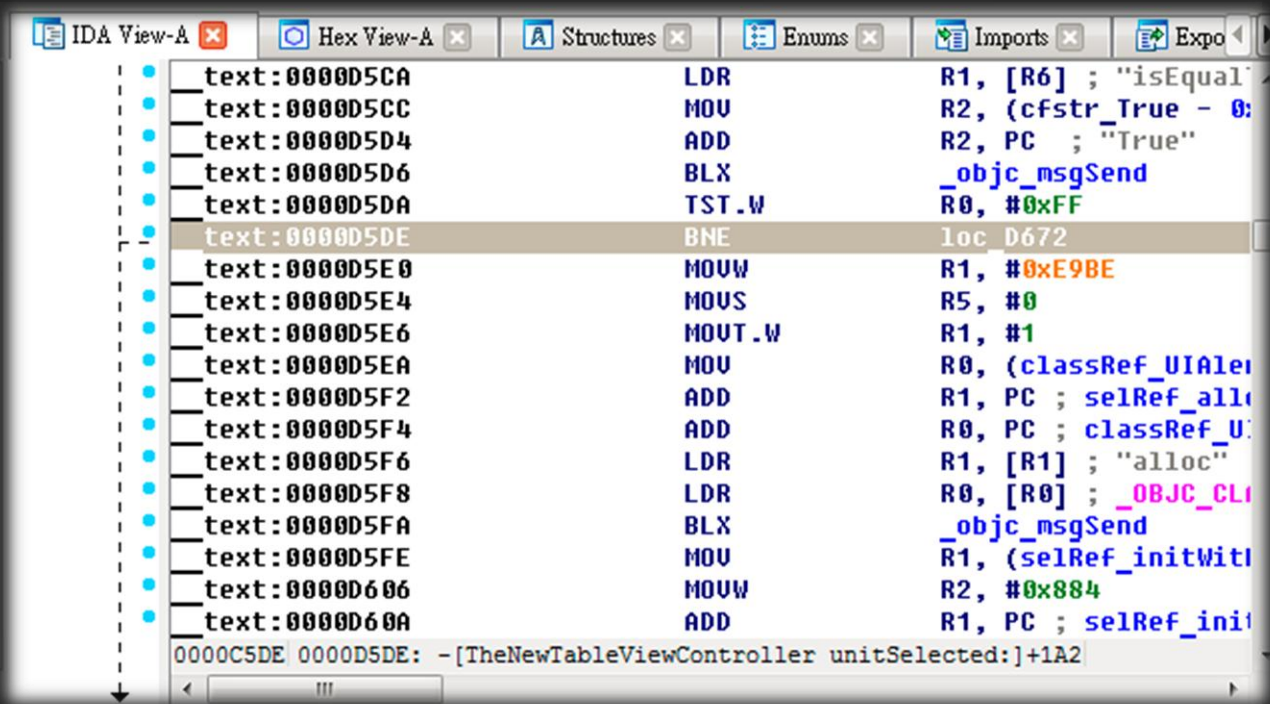


iOS Apps 加密還原 (5)



iOS Apps 加密還原 (6)

Done



```
IDA View-A  Hex View-A  Structures  Enums  Imports  Expo
text:0000D5CA LDR R1, [R6] ; "isEqual
text:0000D5CC MOV R2, (cfstr_True - 0:
text:0000D5D4 ADD R2, PC ; "True"
text:0000D5D6 BLX _objc_msgSend
text:0000D5DA TST.W R0, #0xFF
text:0000D5DE BNE loc_D672
text:0000D5E0 MOVW R1, #0xE9BE
text:0000D5E4 MOVS R5, #0
text:0000D5E6 MOVW R1, #1
text:0000D5EA MOV R0, (classRef_UIAler
text:0000D5F2 ADD R1, PC ; selRef_allo
text:0000D5F4 ADD R0, PC ; classRef_U
text:0000D5F6 LDR R1, [R1] ; "alloc"
text:0000D5F8 LDR R0, [R0] ; _OBJC_CL
text:0000D5FA BLX _objc_msgSend
text:0000D5FE MOV R1, (selRef_initWith
text:0000D606 MOVW R2, #0x884
text:0000D60A ADD R1, PC ; selRef_init
0000C5DE 0000D5DE: -[TheNewTableViewController unitSelected:]+1A2
```

玩弄 iOS Apps

記憶體修改

檔案修改

繞過 IAP 檢查

0x02:

The Profit Part

Memory Patching

Binary Patching

IAP Bypass

最新
上架



旅遊
飲食



投資
理財

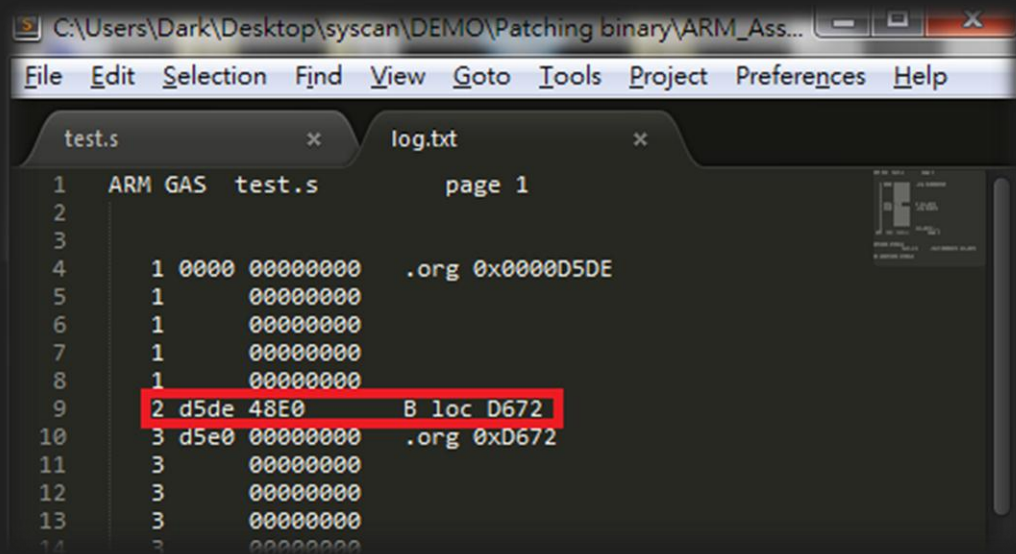


測試目標

記憶體修改

(Demo)

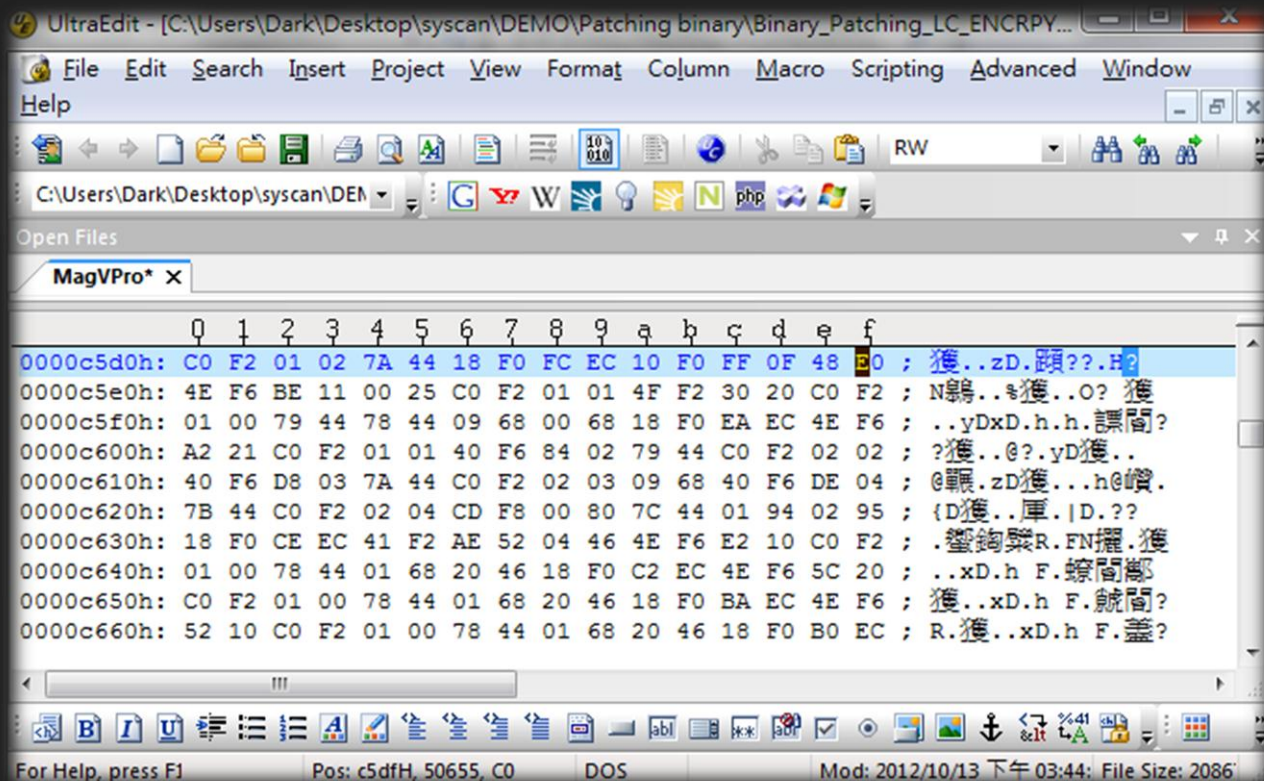
檔案修改 (1)



```
C:\Users\Dark\Desktop\syscan\DEMO\Patching binary\ARM_Ass...
File Edit Selection Find View Goto Tools Project Preferences Help

test.s x log.txt x
1 ARM GAS test.s page 1
2
3
4 1 0000 00000000 .org 0x000D5DE
5 1 00000000
6 1 00000000
7 1 00000000
8 1 00000000
9 2 d5de 48E0 B loc D672
10 3 d5e0 00000000 .org 0xD672
11 3 00000000
12 3 00000000
13 3 00000000
14 3 00000000
```


檔案修改 (2)



檔案修改 (3)

127.0.0.1 [102x31]

Connection Edit View Window Option Help

```
Darks- iPhone:/var/mobile/AppLinks/MagVPro.app/MagVPro.app root# chmod +x MagVPro  
Darks- iPhone:/var/mobile/AppLinks/MagVPro.app/MagVPro.app root# ldid -S MagVPro  
Darks- iPhone:/var/mobile/AppLinks/MagVPro.app/MagVPro.app root#
```

檔案修改 (4)

Done



繞過 IAP(In-App-Purchase)

MITM SSL Proxy

不需要 JB

iOS 6 已經修正這個弱點

Patching IAP API

需要 JB

transactionState

SKPaymentTransactionStatePurchasing
SKPaymentTransactionStatePurchased
SKPaymentTransactionStateFailed
SKPaymentTransactionStateRestored

IAP 檢查流程

```
(void)paymentQueue:(SKPaymentQueue *)queue updatedTransactions:(NSArray *)transactions
{
    for (SKPaymentTransaction *transaction in transactions)
    {
        switch (transaction.transactionState)
        {
            case SKPaymentTransactionStatePurchased:
                if([self putStringToItunes:transaction.transactionReceipt]){
                    // 開發者常常寫到這邊就認為已經完成 IAP 手續, 忽略了 Receipt 檢查
                }
                break;
        }
    }
}
```

繞過 IAP

(Demo)



0x03:

The Fun Part

iOS RAT

Super Gamer

iOS 後門與遠端操控

(Demo)



實作遠端操控

基本上就是 Unix socket programming

關閉螢幕造成 TCP 連線中斷

持續送 heartbeat 封包至 server.

啟動

launchctl load /System/Library/LaunchDaemons/xxx.plist

遊戲大神

(Demo)



結論

iOS Hacking



Techniques and
Tricks

For Profit



How bad it
could be

For Fun



Demonstrated
the possibilities



Thank you!

{dark,tt}@chroot.org